

---

# MAAWG BEST PRACTICES FOR THE USE OF A WALLED GARDEN

## Criteria for Exit and Entry, Remediation and Subscriber Education

### Introduction

As subscriber-originating network abuse increases, Internet Service Providers (ISPs) have been required to enforce more proactive measures in an effort to protect their networks and the traffic originating wherefrom. “Bots” and bot networks (“botnets”) have become an increasingly popular mechanism for spammers and hackers to abuse the network through the propagation of spam, viruses and other forms of malware. This malware is surreptitiously planted on subscribers’ personal computers without their knowledge and as a result end-user subscribers are overwhelmingly targeted as the unwitting accomplices in these malicious networks.

In an effort to reinforce the MAAWG mission to preserve electronic messaging from online exploits and abuse, the MAAWG Botnet/Zombie Subcommittee recommends the following best practices as they relate to the implementation of a walled garden. A walled garden refers to an environment that controls the information and services that a subscriber is allowed to utilize and what network access permissions are granted. The primary goal of these practices is to help end-users become aware of and remove unwanted programs or malware residing on their personal computers and to stop the network from being used for abusive purposes. Unless stated otherwise, all recommendations are the responsibility of the ISP to implement.

The uses and definitions of key words like MUST, SHOULD and MAY used throughout this document are to be interpreted as described in [RFC 2119](#).

### I. Criteria for Exit And Entry To/From Walled Garden Must Be Concise

In an effort to educate users to the risks and issues associated with a malware infected personal computer, ISPs MAY implement a walled garden for new user accounts or any account that they deem as being risky or generating suspicious traffic. The entry and exit criteria for the walled garden must be clear and concise so that it can be understood by the end user.

#### **Recommendations Summary:**

- a) MUST provide a clear notification of the suspected problem; e.g., using the network outside of the Acceptable Use Policy (AUP). MUST also provide an explanation for the notification and an overview of the recommended process to remediate or clean the computer of malware.
- b) MAY redirect HTTP [80] to the appropriate quarantine Web address or Web site respectively.

- c) MAY redirect botnet command and control traffic to a honey network for analysis.
- d) SHOULD manage all outbound SMTP [25] to a quarantine area or honey pot Message Transfer Agent (MTA).
- e) SHOULD allow instant escape based on trust. Trust can be asserted through an action that indicates a clean personal computer or a request to use the network “as is” for a configurable period of time.
- f) MAY provide exit if certain ISP-approved clean-up or security software is downloaded and installed.
- g) The ISP MAY use internal subscriber reputation metrics (determined using detection techniques such as content filters, deep packet inspection, and behavior usage patterns) to trigger entry or exit events from the walled garden.
- h) The ISP MAY use technologies to automatically identify the subscriber’s security posture as advertised by installed and trusted subscriber client software.

## II. Remediation Experience Must Be Convenient to the End User

As ISPs continue to make efforts to protect their networks and subscribers from malicious abuse, it is important for ISPs to do this in a way that is not unreasonably cumbersome to the end user. In order to recoup the investment, the ISP MAY also choose to make remediation tools available at a cost to the end user. Those tools MUST be made available via a means that is consistent with the ISP’s typical support environment. Additionally, the walled garden MUST allow access to Web sites so that the end user can download critical, applicable software updates and patches, either through direct access or via indirect proxy connection mechanisms. (This presents the possibility of the provider or the contracted ASP offering remediation via a single portal, like Microsoft does with its Windows Update and the multiple new driver downloads it initiates on your behalf.)

### **Recommendations Summary:**

- a) MUST be able to provide either free and/or fee-based remediation alternatives (or links to existing online tools).
- b) MUST present recognizable information that legitimizes the experience as an official ISP Notice and Remediation Process. Examples of this information include data such as an account number or secret question answer.
- c) MUST provide details on how to contact customer support for assistance.
- d) SHOULD not require a reboot of the end user’s personal computer for remediation experience to take effect.
- e) MUST provide links to URLs and domains that help resolve the unwanted condition with OS patches and security updates (if appropriate).
- f) SHOULD provide “Click to Chat with Customer Support” or a third-party providing customer service on behalf of the ISP.
- g) SHOULD provide ISP support or abuse contact information (e.g. phone number).
- h) SHOULD instruct customers sending malicious SMTP [25] traffic to reconfigure Mail User Agents (MUAs) to send outbound email traffic over port 587.

- i) SHOULD present unique remediation experiences depending on the unwanted condition and past user actions, i.e. a user SHOULD see an experience that provides a fix for the exact problem or type of malware suspected.
- j) SHOULD provide a security client that is minimally intrusive; downloads quickly; easily installs without conflicting with other application software, such as an already configured security client; does not require a reboot; and does not require a full scan of the computer to detect and remove malware.
- k) MUST allow for redirection exceptions so that the user is permitted to utilize emergency online services

### **III. End-User Education Should Be a Primary Focus**

Since the end user is typically the weak link in the security chain the ISP SHOULD make reasonable efforts by way of documentation available on their Web site so that the end user can proactively educate themselves on how to mitigate risk of malware infection. As such, documentation in the form of FAQs, support videos, tutorials, and a searchable knowledge base SHOULD be made available to the end user. If provided, these materials MUST be made available to the end user via a method that is consistent with the look and feel of the ISP's customer service interface. Additionally, the available documentation SHOULD be broad enough to cover applications across several different types of Internet technologies and across several different types of computer OS (e.g. Windows, MacOS, Linux).

#### **Recommendations Summary:**

- a) MUST present recognizable information that legitimizes the experience as an official ISP Notice and Remediation Process. Examples of this information include data such as an account number or secret question answer.
- b) SHOULD provide intuitive user education via FAQs and tutorials.
- c) SHOULD provide alternative learning center tools such as a simple video greeting and search knowledge centers.
- d) SHOULD provide educational information for multiple types of applications including email (POP3/SMTP) and browsing (HTTP).